Coding Theory

Lecture Projection

Kit Tyabandha, PhD

Mahidol University

Thailand

27th February, 2006

Preface

This work began in October 2005 when I started teaching Coding Theory. Coding and cryptography are similar, but the main concern of the former is in the existence of a noisy environment whereas that of the latter is in the secrecy of the message from unintended party. The concept of entropy, being fundamental for the purposes of economy, privacy and reliability, play a role in all branches of both subjects.

In this course the main theme is coding theory. Cryptography was only mentioned briefly towards the end. As the students were fairly familiar with algebra, but had familiarity with neither finite fields nor polynomial rings, we had some practice sessions where the students tried their hands on problems. In all we had two practices, on 6 and 13 January, three quizzes, on 20 January, 3 and 10 February, and one midterm exam on 27 January 2006. Our final exam was on 23 February 2006.

These projections were adapted from the hand-outs given to students for the lecture. Both are written on plain TEX. I stopped making projection after the lecture on Linear Code on 9 December 2005. The reason was because the nature of activities we did in class had changed. We spent a fair amount of our time doing the exercises and problems, so the lecturing was shortened. And since the students were by now more familiar with the subject, I needed only guide them through the hand-outs. Another reason was because I felt that I had been producing too many of them, so I did not want to waste more paper. To do a similar thing for other subjects in the future it would probably do well to limit the number of these projections to under 20 pages for each lecture.

Apart from this Lecture Projection I also plan to compile for this subject a Lecture Hand-outs, which would be more detailed than the present work, and a Lecture Notes in the form of a book. I thank my students for allowing me the privilege of teaching them. I hope they have learnt from me as much as I have from them.

Kit Tyabandha, PhD

Mahidol University
Bangkok, Thailand

kippuc@gmail.com

27^{th} February, 2006

Table of contents

Course Syllabus

Programme of study:	Bachelor of Science in Mathematics	**Faculty:**	Science
Course Title:	Coding Theory	**Course Code:**	SCMA 360
Number of Credits (Lecture–Lab):	3(3–0)	**Type of Course:**	Specialised
Academic Year and Semester:	2005, Second Semester	**Instructor:**	Dr Kit Tyabandha

Course Objective

To introduce the students to the theory of coding, namely the basic principles behind it, as well as its main mathematical ingredients and uses. The students should be able to pursue doing a research in this field, had they a wish to do so in the future.

Course Description

In this course we learn about the theory of coding together with some basic principles of cryptography and cryptology. Firstly we study about error, entropy and bounds in coding, then about group, field and finite field. Next we look at various types of coding, namely linear, cyclic, Bose-Chaudhuri-Hocquenghem, Goppa, and maximum distance separable codes, and also if we have enough time Hadamard and quadratic residue codes. Historical development of conceptions of fundamental concepts and the various codes is briefly mentioned, as also the relationship among the different types of code. And then we mention briefly some basic ideas in cryptography in the light of coding.

Course Outline

Week	*Date*	*Topic of lecture*	*Hours*
1	28 October 2005	Error and distance	3
2	4 November 2005	Entropy and mutual information	3
3	11 November 2005	Group, field and finite field	3
4	18 November 2005	Bounds in coding	3
5	25 November 2005	Group-, polynomial-, and Hamming codes	3
6	2 December 2005	Finite field- and BCH codes	3
7	9 December 2005	Linear codes	3
8	6 January 2006	Cyclic codes	3
9	13 January 2006	Goppa codes	3
10	20 January 2006	MDS code	3
11	10 February 2006	Cryptography	3

Teaching method

There were lectures and practices in class. All practice exercises, quizzes and exams were done in an opened-book manner. These questions were of various nature. There were those that could be done by studying some examples given, demonstration and proof, defining terms and jargons, and also writing technical essay on a given topic.

Teaching media

A camera projector and a microphone were the hardware media used. The material used as a media were lecture projections in this collection and lecture hand-outs, which will go into another collection.

Evaluation methods

means	*per cent*
Attendance	10
Practice and exercise	10
Quiz 1	10
Quiz 2	10
Quiz 3	10
Midterm exam	20
Final exam	30

Since the subject as well as the exams were rather difficult, evaluation will be based on relative performance among the students rather than on preassigned grading steps.

Bibliography

R C Bose and D K Ray-Chaudhuri. On a class of error-correcting binary group codes. *Inform. Control.* **3**, 68–79, 1960

Solomon W Golomb, Robert E Peile and Robert A Scholtz. *Basic concepts in information theory and coding, The adventures of Secret Agent 00111.* Plenum Press, New York, 1994

V D Goppa. A new class of linear error-correcting codes. *Probl. Peredach. Inform.* **6**, 3, 24–30, 1970

V D Goppa. Rational representation of codes and (L, g) codes. *Probl. Peredach. Inform.* **7**, 3, 41–9, 1971

D Gorenstein and N Zierler. A class of cyclic linear error-correcting codes in p^m symbols. *J. Soc. Ind. App. Math.* **9**, 107–214, 1961

H J Helgert. Alternant codes. *Information and Control.* **26**, 369–80, 1974

Raymond Hill. *A first course in coding theory.* Clarendon, 1986

A Hocquenghem. Codes correcteurs d'erreurs. *Chiffres.* **2**, 147–56, 1959

San Ling and Chaoping Xing. *Coding theory, a first course.* Cambridge University Press, 2004

F J MacWilliams and N J A Sloane. *The theory of error-correcting codes.* North-Holland, Amsterdam, 1977

Robert J McEliece *The theory of information and coding.* Addison-Wesley, 1977

M Plotkin. Binary codes with specified minimum distance. *IRE Transaction on Information Theory.* **6**, 445–50, 1960

I S Reed and G Solomon. Polynomial codes over certain finite fields. *J.Soc.Ind. App. Math.* **8**, 300–4, 1960

Bruce Schneier. *Applied cryptography.* John Wiley & Sons, 1994

George F Simmons. *Topology and modern analysis.* McGraw-Hill, 1963

L R Vermani. *Elements of algebraic coding theory.* Chapman & Hall, 1996

Dominic Welsh. *Codes and cryptography.* Oxford, 1988